U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: National Conservation Training Center Property Management System
Bureau/Office: U.S. Fish and Wildlife Service
Date: July 21, 2020
Point of Contact:
Name: Jennifer L. Schmidt
Title: Associate Privacy Officer
Email: FWS_Privacy@fws.gov
Phone: (703) 358-2291
Address: 5275 Leesburg Pike, MS: IRTM Falls Church, VA 22041-3803

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The National Conservation Training Center (NCTC) is a facility that provides exemplary training and professional development to U.S. Fish and Wildlife Service (FWS) employees and conservation partners from Federal, Tribal, state, and local governments, non-governmental organizations and private institutions such as research firms and universities in support of the FWS mission to work with others to conserve, protect, and enhance fish, wildlife, plants and

their habitats for the continuing benefit of the American people. On a daily basis, NCTC hosts approximately 200 overnight guests at its campus in Shepherdstown, West Virginia, about 30% from non-Federal agencies. NCTC uses the Property Management System (PMS), a third-party, Commercial off the Shelf (COTS) product, to manage hotel services such as guest registration, check-in and payment. PMS is a property management system that provides NCTC with tools needed by a limited-service hotel operation such as quick reservation function, one-key check in, and simple cashiering functionality.

C. What is the legal authority?

5 U.S.C. § 4101, et seq., Government Organization and Employees Training; Executive Order 11348, Providing for Further Training of Government Employees, as amended by Executive Order 12107, Relating to Civil Service Commission and Labor Management in Federal Service; 5 CFR Part 410, Training; and Americans with Disabilities Act, 42 U.S.C. 12101.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

☒ No: TBD – PMS is in the process of CSAM registration.

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None.		**Not applicable.**	

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: INTERIOR/DOI-16, Learning Management System (LMS) (October 9, 2018) 83 FR 50682.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: This collection will come under DOI's Learning Management System "DOI Talent," for which the Department currently seeks OMB approval.

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Group Affiliation
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Emergency Contact
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other: *Describe*

Username and password of authorized PMS users who are all Aramark contractors, with the exception of the System Administrator.

All guests are asked when the reservation is confirmed if they have any special requests including disability accommodations or dietary needs. Medical or health information collected from all guests may include service animal accompaniment, allergies and sensitivities including cleaners, linens and food. Dietary requirements such as vegan, celiac, diabetic, etc. are shared with NCTC Chef. Guests may relay any other health related problems or needs that they feel the

NCTC should be aware of. It is also asked upon check in if anyone will need assistance in the event that there is an emergency.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☐ Web site
☐ Fax
☒ Telephone Interview
☐ Information Shared Between Systems *Describe*
☒ Other: *Describe*

Once an individual is notified that he or she is accepted for class enrollment, the individual must call NCTC Reservations to confirm his or her lodging room and provide payment information, if necessary. For sponsored training events coordinated through DOI Talent, the Meeting Planner from the NCTC Scheduling & Events Management team, downloads the participant list from DOI Talent and provides it to the NCTC Front Desk contractor to manually transcribe guests' PII (name, affiliation, and email address) into PMS. The training sponsor notifies the guests that they need to call NCTC Reservations and confirm their information and the dates of their stay. After calling to make the initial reservation, the guest may call or email NCTC Reservations to cancel or make any changes to an existing reservation. During check-in, the NCTC Front Desk will retrieve the guest's reservation using his or her name or reservation confirmation number. PMS users (NCTC Guest Services contractors) confirm guests' reservations via email and provide receipts upon checkout on paper forms or via email, depending on guest preference.

D. What is the intended use of the PII collected?

The PII is used to grant authorized access to PMS; to provide lodging and other guest services to NCTC students and guests; and to facilitate payment as necessary for these services.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

In the ordinary course of business PII is not shared beyond Guest Services; however, PII may be shared with FWS employees and NCTC contractors who have a need-to-know in the performance of their official duties.

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

Aramark is the FWS-contracted vendor for all NCTC guest services. In the ordinary course of business, PII will be shared among authorized Aramark contractors working for NCTC Guest Services who have a need-to-know in the performance of their official duties to facilitate communication with guests and payments for lodging.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individual guests voluntarily provide the requested PII in order to reserve or confirm a room and stay overnight at NCTC. Individuals may decline to provide their PII; however, they will not be able to reserve a room. PMS users voluntarily provide their PII during the onboarding process in order to be granted authorized access to FWS systems, including PMS; and perform their official duties. Contractors who decline to provide the requested PII will not be able to complete the onboarding process at the Service or perform their official duties.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

The Privacy Act statement for PMS will be posted at the NCTC Front Desk. Reservation agents and Front Desk staff may read the statement over the phone to guests upon request.

☒ Privacy Notice: *Describe each applicable format.*

The bottom of NCTC's webpages include a "Privacy" hyperlink to FWS' Privacy and Other Web Policies. Authorized users of U.S. Government systems, including PMS, receive a "subject to monitoring" notice upon logging into the system and/or equipment. Notice is provided through the publication of this PIA, and the INTERIOR/DOI-16, which may be viewed at https://www.doi.gov/privacy/sorn.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data will be retrieved by the guest's name or reservation confirmation number, or by the PMS authorized user's username and password.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*

☒ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

The PII will be collected directly from the guest over the phone while reserving a room or confirming an existing reservation (for sponsored training events) and is therefore presumed to

be accurate; however, the contact information will be repeated over the phone by the reservation agent to the guest for verification. The credit card information will be verified when it is run for payment by the agent. If the credit card cannot be processed, the agent will make sure the details have been recorded accurately and run again. For returning guests, the agent will verify that the guest wants to use the credit card "on file," or if the guest wishes to use a different credit card – in which case the agent will replace the previous credit card information. The guest reservation agent will also check for any needed updates or changes to the guest's profile.

B. How will data be checked for completeness?

The PII will be collected directly from the guest over the phone while reserving a room or confirming an existing reservation (for sponsored training events) and is therefore presumed to be accurate; however, the contact information will be repeated over the phone by the reservation agent to the guest for verification. The credit card information will be verified when it is run for payment by the agent. If the credit card cannot be processed, the agent will make sure the details have been recorded accurately and run again. For returning guests, the agent will verify that the guest wants to use the credit card "on file," or if the guest wishes to use a different credit card – in which case the agent will replace the previous credit card information. The guest reservation agent will also check for any needed updates or changes to the guest's profile.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

The PII will be collected directly from the guest over the phone while reserving a room or confirming an existing reservation (for sponsored training events) and is therefore presumed to be accurate; however, the contact information will be repeated over the phone by the reservation agent to the guest for verification. The credit card information will be verified when it is run for payment by the agent. If the credit card cannot be processed, the agent will make sure the details have been recorded accurately and run again. For returning guests, the agent will verify that the guest wants to use the credit card "on file," or if the guest wishes to use a different credit card – in which case the agent will replace the previous credit card information. The guest reservation agent will also check for any needed updates or changes to the guest's profile.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Agency-sponsored training records for PMS are maintained under the Departmental Records Schedule (DRS) 2.1, Short-term Human Resources Records (DAA-0048-2013-0001-0004), which was approved by the National Archives and Administration (NARA). These records have a temporary disposition and are cut-off as instructed in the agency/bureau records manual, or at

the end of the fiscal year in which the record is created if no unique cut-off is specified. Records are destroyed 3 years after cut-off.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There are moderate privacy risks to individuals from the amount and types of PII collected and stored in PMS. The primary privacy risks are unauthorized access, unauthorized disclosure and misuse of the data in the system. To mitigate these risks the NCTC has implemented several controls and best practices.

Only authorized NCTC employees and contractors with guest services responsibilities may be granted PMS access and are allowed to input or change data in PMS. PMS features an auditing trail which the System Administrator can use to identify any unauthorized access or change to the system. Access to PMS is limited to NCTC employees and contractors who have completed the required security and privacy awareness training, signed the DOI Rules of Behavior acknowledging their security and privacy responsibilities, and have a need-to-know in the performance of their official duties. NCTC contractors also must agree to the contract's Non-Disclosure Agreement (NDA) before receiving access to the Service's network. Once a NCTC contractor is granted FWS network access and his or her Active Directory account is created, the PMS System Administrator will approve his or her PMS access request.

NCTC collects the minimum PII necessary to facilitate guests' stays and payments. NCTC includes the individual in the collection process by collecting the PII directly from him or her over the phone during the reservation process. If the guest's stay is funded by the Department or another organization, the individual must call the NCTC to verify their contact information and confirm the dates of their stay. This helps to ensure the accuracy, relevancy and completeness of the PII collected. While many guests of NCTC return periodically, there is a risk that credit card information will be maintained for longer than necessary. To mitigate this risk, the NCTC will not store, or will delete the credit card information from a guest's profile, upon request.

Health or medical information that guests may provide is accessible on a limited, role-based need. Guest Service Agents are trained to understand the importance of keeping medical and special needs information confidential and to record only information relevant to operations. For

example, if a guest requests a refrigerator to keep insulin in, the housekeeping record only reflects the refrigerator request.

These privacy risks are mitigated by technical controls as well. The PMS has undergone a formal Assessment and Accreditation and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. PMS is rated as Moderate based on the type of data and it requires the Moderate baseline of security and privacy controls to protect the confidentiality, integrity and availability of the PII contained in the system. PMS has developed a System Security and Privacy Plan (SSPP) based on NIST guidance and is a part of the FWS Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with DOI policy and standards.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

PMS is a property management system that provides NCTC with tools needed by a limited-service hotel operation such as quick reservation function, one-key check in, and simple cashiering functionality, and the use of personal data within is both relevant and necessary to the use of the system.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☐ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

The PMS contractors must complete the Department's mandatory information security and privacy training courses, and sign the contract's Non-Disclosure Agreement (NDA) before receiving access to the Service's network. Once a contractor is granted FWS network access and his or her Active Directory account is created, the PMS System Administrator will approve his or her PMS access request, as necessary for the performance of the contractor's official duties. PMS access is limited to authorized Aramark contractors with guest services responsibilities. Only these contractors may input or change data in PMS.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Aramark's contract with NCTC includes the required Federal Acquisition Regulation (FAR) clauses for systems that handle PII.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*

☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

Not applicable. This system does not have the capability to monitor individuals.

M. What controls will be used to prevent unauthorized monitoring?

Not applicable. This system does not have the capability to monitor individuals.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices

☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The PMS Information System Owner is the official responsible for oversight and management of the PMS security controls and protection of information processed and stored by PMS. The Information System Owner, Information System Security Owner, and Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy and provide adequate notice, making decisions on the Privacy Act requests for notification, access and amendment, as well as processing complaints, in consultation with the FWS Associate Privacy Officer. These officials and authorized PMS users are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting requirements of the Privacy Act and other Federal laws and policies for the data managed, used and stored in PMS.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The PMS Information System Owner is the official responsible for oversight and management of the PMS security controls, and for ensuring to the greatest extent possible that PMS agency data is properly managed and that access to data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of data is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures. In accordance with the Federal Records Act, the FWS Records Officer is responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.